NORTH CAROLINA
STATE BOARD OF ELECTIONS

VIA EMAIL
VR Systems, Inc.
Mindy Perkins, Chief Executive Officer
c/o Michael L. Weisel, Esq.

April 18, 2019

Re: Request for assurance regarding network and product security.

Dear Ms. Perkins:

I write seeking immediate assurance by VR Systems, Inc. ("VR Systems") regarding the security of its network and the electronic poll book product marketed as "EViD." The U.S. Department of Justice today released a redacted copy of the *Report on the Investigation into Russian Interference in the 2016 Presidential Election* by Special Counsel Robert S. Mueller III (the "*Report*"). Today's release follows the July 2017 indictment against 12 Russian nationals for their alleged roles in computer hacking conspiracies aimed at interfering in the 2016 U.S. elections (the "*Indictment*"). *U.S. v. Viktor Borisovich Netyksho, et al* (1:18-cr-215, District of Columbia).

The Special Counsel's Report and Indictment state that Russian cyber actors in 2016 targeted a vendor of software systems used to verify voter registration information—identified as "Vendor 1" in the *Indictment*[1] and in redacted form [PP [redacted]] in the *Report*.[2] Specifically, today's *Report* indicates that Russian intelligence successfully "installed malware on the company network," which "permitted the GRU to access the infected computer," along with "at least one Florida county government."[3]

[1] *See e.g.*, *Indictment* at Paragraphs 73 through 76.
[2] *See e.g.*, *Report* at 50 through 51.
[3] *Id* at 51.

In your legal action against our Agency, *VR Systems, Inc. v. State Board*, 17 BOE 7136 (dismissed), your company served responses to discovery in March 2018, including the following:

> 8. Have you ever experienced a breach of security regarding EViD, including but not limited to unauthorized access to the code of EViD, voter data, voting data, or personally identifiable information?
>
> **ANSWER:**
>
> **No**

In response to Interrogatory No. 9, asking that you describe how VR Systems would know whether a breach or successful phishing attack occurred, the company responded as follows:

> **If a breach or successful phishing attack were to occur, the remnants of the attack could be detected through unauthorized access to the network, unauthorized changes to data on the network, or by the detection of a virus that had been placed on the network during a breach.**

VR Systems went on to describe its investigation into the "Russian spear phishing campaign" in 2016, by responding to Interrogatory No. 11 as follows:

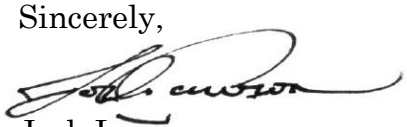
> **An email was sent to the staff, warning of the suspicious email and then the address and the suspicious emails were quarantined within the VR Systems email system. VR Systems then interviewed all the intended recipients of the suspicious emails and validated that none had opened the attachment.**

The response to Interrogatory No. 11 went on to explain that "[t]his failure by the cyber actors prevented any access to genuine VR System's [*sic*] email or password information," and the response to Interrogatory No. 24 states "[t]o VR Systems's knowledge, EViD has never been hacked."

Our Agency understands that information continues to come to light regarding aggressive cyber operations against the United States during the 2016 election cycle; we are sympathetic to the possibility that VR Systems has gained new information since March 2018; and it is possible that you may represent that VR Systems is not the vendor referenced in the *Indictment* or today's *Report*.

The Agency requests that VR Systems provide immediate, written assurance regarding the security of your network and the EViD product by ***(1)*** confirming whether VR Systems or its agent is "Vendor 1" referenced in the *Indictment* at Paragraph 73 and/or in the Report at page 51 as the "voting technology company that developed software . . . to manage voter rolls"; ***(2)*** indicating whether VR Systems believes its responses to discovery remain accurate, given any new information it has received; and ***(3)*** providing representations to the State Board of Elections regarding the present security of VR Systems' network and the EViD product. Please provide your response to legal@ncsbe.gov. Thank you for your prompt attention to this matter.

Sincerely,



Josh Lawson
General Counsel